REMARKS

This Amendment Under 37 C.F.R. §1.116, is in response to the final Office Action mailed March 24, 2006. A Request For Continued Examination (RCE) is filed on even date herewith, together with all requisite fees.

Independent Claims 9 and 15

In the final Office Action, claims 9-13 and 15-19 were rejected under 35 U.S.C. §102(e) as being anticipated by Brown et al. (U.S. 2004/0139327 A1). Reconsideration and withdrawal of these rejections are respectfully requested.

Claim 9 has been amended to recite:

> validating the authority information included within the received certificate by accessing a store of authority information **that is coupled to the network and** that is independent of the received certificate **and by matching the authority information included within the received certificate to authority information that is associated with the user and that is stored in the accessed independent store of authority information**, and

Similarly, claim 15 has been amended to recite:

> authorization validating code configured to enable validation of the authority information within the received certificate against corresponding authority information for the user stored in a data structure **that is coupled to the network and** that is independent of the received certificate **by accessing the data structure over the network and by matching the authority information included in the received certificate to the corresponding authority information stored in the accessed data structure**.

In support of its rejection, the Office points to Figs. 1, 2, 3 and 8 and to paragraphs 0165, 0174, 0183 and to claim 80. However, none of these figures, passages or claim teaches to validate the authority information in the received certificate with corresponding authority information that is stored in a store or data structure that is accessed over the network and that is independent of the received certificate for any purpose, and much less for the purpose of matching the authority information in the received certificate to corresponding authority information stored in the accessed store/data structure.

In fact, Brown et al.'s paragraph 0165 only mentions that the digital certificate includes "information about the subscriber and his authority to conduct certain transactions. No mention is made of any store or data structure that is independent of the certificate and that stores corresponding authority information. In fact, paragraph 0174 specifically states that the request is authorized based on the authority of the signer – which authority, Brown et al. teach us, is contained in the certificate itself. No matching of authority information is carried out as is presently claimed. Paragraphs 0183 and 0184 are even more on point here:

> **[0183] If, however, the signature was successfully verified, the method continues by checking 886 the digital certificate corresponding to the signature 118 for the maximum signing authority of the signer. Under X.509 version 3, the digital certificate may specify a maximum signing authority. For example, a signer may only be authorized to digitally sign payment requests up to $1000.00. Thus, the digital certificate of the signer will indicate a maximum signing authority of $1000.00.**
>
> **[0184] A determination 888 is then made whether the amount of the electronic payment request is authorized, i.e. the payment amount does not exceed the signer's maximum signing authority. If not, the method continues with step 890 by processing the authorization failure. In one embodiment, an authorization failure may simply result in the payment request being ignored, in which case the signer may be billed for the deficiency. However, in alternative embodiments, the signer and/or the signer's employer, bank, or the like, will be notified of the authorization failure.**

Therefore, Brown et al. teach to compare the amount of the payment request with the amount of the signing authority in the digital certificate to determine whether the request should be authorized. Brown et al. do not teach to access a data structure or store of authority information that is independent of the certificate. Brown et al. do not teach matching the authority information in the certificate with corresponding authority information obtained by accessing the independent store of authority information over the network. The tags (to-be-signed tag, accessible tag and role tag) in Brown et al. noted by the Examiner are contained in the certificate itself, as is the information (values) identified and framed by these tags:

> **[0095] In one embodiment, the accessible-by tag 120 includes an indication of one or more roles, access levels, or the like, of individuals who may view and/or modify the document 102. For example, an accessible-by tag 120 has the following format in one embodiment:**

3 <AccessibleBy> <ViewModify><Per- sInfo Role="Judge"></ViewModify> <View><PersInfo Role="Plaintiff"></View> . . . </AccessibleBy>

[0096] In this example, the judge may both view and modify the document 102, while the plaintiff may only view the document 102. Preferably, all other individuals would not be able to view or modify the document.

Thus, the information identified by the tags; namely, judge, plaintiff etc. is contained within the certificate itself, framed by the beginning <> and ending </> tags – and not in a store or data structure that is independent of the digital certificate and accessed over the network, as claimed herein. Brown et al., therefore, cannot anticipate claims 9 and 15 or any of their respective independent claims. Reconsideration and withdrawal of the 35 USC §102(e) rejections are, therefore, respectfully requested.

Independent claims 1 and 29

Claims 1-8 and 29-33 are rejected under 35 U.S.C. §103(a) as being unpatentable over Brown et al. in view of Hwangbo (U.S. 2003/0154376 A1). Reconsideration and withdrawal of the 35 USC §103(a) rejections are, therefore, respectfully requested.

Claim 1 is amended as follows:

> and wherein the second code portion of the digital certificate is configured to define an authority of the user of the client computer to request that the server computer carry out the requested action, the second code portion being configured for inclusion within the extension field of the first code portion, the authority of the user defined within the second code portion of the certificate being verifiable by the server computer independently of the digital certificate by accessing**, over the network,** a store of authority information that is independent of the digital certificate **and by matching the authority of the user defined within the second code portion of the certificate to corresponding authority information of the user retrieved from the accessed independent store of authority information**.

Similarly, claim 29 is amended as follows:

> ~~and~~ wherein the second code portion of the digital certificate is configured to define an authority of the user of the client computer to request that the server computer carry out the requested action, the second code portion being configured for inclusion within the extension field of the first code portion, the authority of the user defined within the second code portion of the certificate defining access rights of the user to data and programs within the computing environment**, and**
>
> **code for accessing, over the network, a store of authority information that is independent of the digital certificate and that stores corresponding**

authority information, the accessing code being configured to match the authority of the user defined within the second code portion of the certifite to the corresponding authority information accessed from the independent store to validate the rights of the user to data and programs within the computing environment.

Therefore, each of the claims 1 and 29 include recitations drawn to matching the corresponding authority information accessed from the independent store of authority information to the authority information in the digital certificate. As has been demonstrated relative to claims 9 and 15, Brown et al. do not teach or suggest any such subject matter. Moreover, this fundamental shortcoming of Brown et al. is not remedied by Hwangbo's teaching of a digital certificate containing a first and second portion, whether such teachings are considered singly or in combination with Brown et al. The applied combination, therefore, cannot teach or suggest the claimed subject matter of either claims 1 and 29 or that of any of their respective dependent claims.

Independent claim 20

Claims 20-28 are cancelled.

Applicant believes that this application is now in condition for allowance. If any unresolved issues remain, please contact the undersigned attorney of record at the telephone number indicated below and whatever is necessary to resolve such issues will be done at once.

Respectfully submitted,

Date: September 25, 2006 By: _____

Alan W. Young
Attorney for Applicant
Registration No. 37,970

Young Law Firm, P.C.
4370 Alpine Rd., Ste. 106
Portola Valley, CA 94028
Tel.: (650) 851-7210
Fax: (650) 851-7232

\\Ylfserver\ylf\CLIENTS\ORCL\5881 (OID-2003-142-01)\5881 AMEND.2.doc